UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

7338 S. Heatheridge Circle, Franklin, WI 53132, to include any outbuildings on the curtilage of the property ("TARGET RESIDENCE"), white BMW bearing Wisconsin license plate number BAC-7291 ("TARGET VEHICLE #1")

Case No. 25 MJ 74

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 842(a)(3)(B)	Distribution of Explosives without an ATF License
18 U.S.C. 842(j)	Illegal Storage of Explosives

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

PAUL KOZELEK Digitally signed by PAUL KOZELEK Date: 2025.06.05 16:44:55 -05'00'

Applicant's signature

Paul G. Kozelek, Special Agent - ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 6/5/2025

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Paul G. Kozelek, being first duly sworn, hereby depose and state as follows:

BACKGROUND

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (hereinafter "ATF"). As such, I am "an investigator or officer charged by the Attorney General with the duty of enforcing any of the criminal, seizure, or forfeiture provisions of the laws of the United States," within the meaning of Section 3051(a) of Title 18, United States Code; that is, an officer of the United States who is empowered by law to conduct investigations of, execute warrants and to make arrests for offenses against the United States and offenses enumerated in United States Code Title 18 and Title 21.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and have been since January of 2020. Prior to my employment with ATF, I was a Sheriff's Deputy with the Jackson County Sheriff's Office in Black River Falls, WI. My duties included patrol, drafting and executing search warrants, and investigations related to state and county criminal violations. Previous to my tenure with the Jackson County Sheriff's Office, I served with the United State Marine Corps from 2004 until 2008, and the United States Marine Corps Reserve from 2011 until 2014. I left the Marine Corps as an E6/Staff Sergeant holding the billet of Platoon Commander. I received my bachelor's degree in Criminal Justice Administration from Viterbo University, La Crosse, WI in 2016.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority.

Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. This affidavit is based upon my personal knowledge as well as information provided to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and my training and experience.

5. I am investigating Luqman Ahmed KATTOUM (KATTOUM), and others known and unknown, who are suspected of violating Title 18, United States Code, Section 842(a)(3)(B) (distribution of explosives without an ATF license); and Title 18, United States Code, Section 842(j) (illegal storage of explosives).

6. I am submitting this affidavit in support of an application for a warrant to search the following location: 7338 S. Heatheridge Court, Franklin, WI 53132, to include any outbuildings on the curtilage of the property, as more fully described in Attachment A (hereinafter "TARGET RESIDENCE"). Your affiant also seeks to search a white BMW bearing Wisconsin license plate number BAC-7291 ("TARGET VEHICLE #1"), more fully described in Attachment A and has been identified as being associated to KATTOUM and/or the TARGET RESIDENCE.

7. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant authorizing the search of the TARGET RESIDENCE and TARGET VEHICLES, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause to believe that the TARGET RESIDENCE and the TARGET VEHICLES contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 842(a)(3)(B) (distribution of explosives without an ATF license); and Title 18, United States Code, Section 842(j) (illegal storage of explosives), as further described in Attachment B.

8. Based upon the information described below, I submit that probable cause exists to believe that Luqman Ahmed KATTOUM (M/W DOB XX/XX/2005), residing at 7338 S. Heatheridge Court, Franklin, WI 53132, Milwaukee County and State and Eastern District of Wisconsin, committed violations of Title 18, United States Code, Section 842(a)(3)(B) (distribution of explosives without an ATF license); and Title 18, United States Code, Section 842(j) (illegal storage of explosives), and that evidence relating to these crimes, more particularly described in Attachment B to the search warrant application, can be found at the Subject Premises.

9. I submit this affidavit for the limited purpose of demonstrating sufficient probable cause for the requested warrant. It does not set forth all of my knowledge about this matter, I have set forth facts that I believe are sufficient to establish probable cause to believe that: (1) on June 4, 2025, the above-named individual distributed or attempted to distribute explosives in violation of Title 18, United States Code, Section 842(a)(3)(B); and (2) evidence, instrumentalities, fruits, and contraband of violations of Title 18, United States Code, Sections 842(j) are located at the TARGET RESIDENCE.

PROBABLE CAUSE

10. On June 5, 2025, your affiant was provided information from the Milwaukee Fusion Center (Fusion) which showed a publicly available Instagram identified as "https://www.instagram.com/habib.mke" offering for sale illegal explosive devices. The apparent owner of the account was identified as Luqman Ahmad KATTOUM (M/W DOB XX/XX/2005). Your affiant observed the following pictures were posted on June 4, 2025:

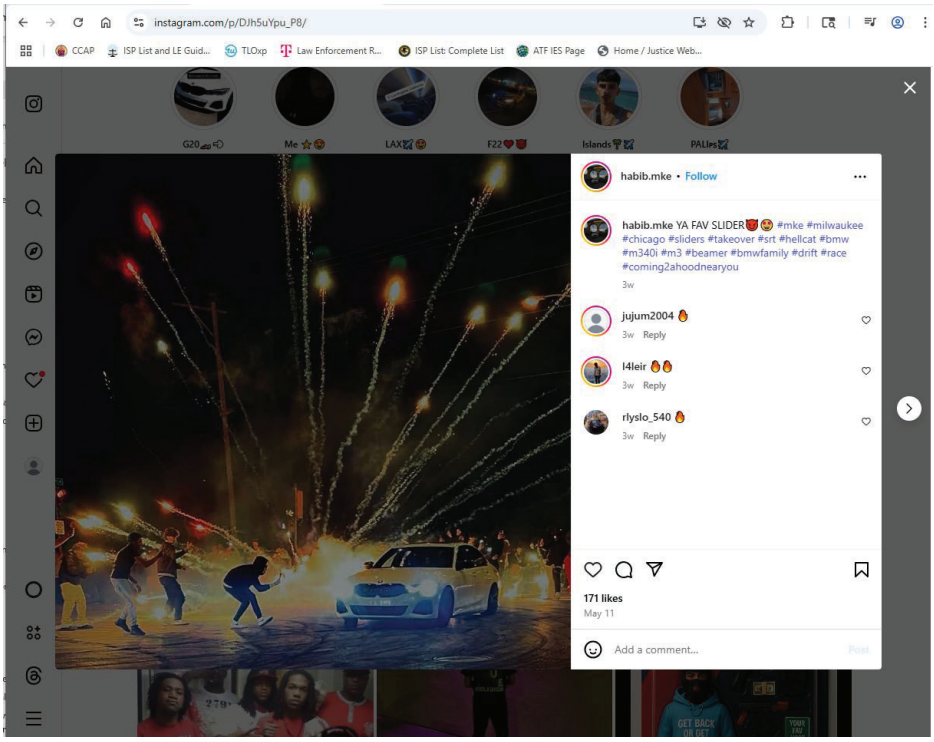
11. A picture showed a hand holding a carboard wrapped item which Your affiant recognized from training and experience as a "mortar shell" type firework. The text stated, "3 INCH MORTAR IFYKYK $50." Your affiant knows that "IFYKYK" is slang for "if you know, you know." This indicated KATTOUM did not want to put the full description of the device on social media. This item is, or appears to be, a commercial explosive and requires a Federal Explosive License to possess and sell issued by ATF.

12. The next picture showed an item similar to that in paragraph 11 above, but larger. The item was labeled "4 INCH MORTAR $80 IFYKYK". Your affiant recognized the item from training and experience as a "mortar shell" type firework. This item is, or appears to be, a commercial explosive and requires a Federal Explosive License to possess and sell issued by ATF.


habib.mke 5h
4 INCH MORTAR
$80
IFYKYK

13. A picture showed carboard wrapped items with common pyrotechnic fuse protruding out the top corner. These items are consistent with homemade devices. The text read "QUARTER STICKS DYNAMITE $10 HALF STICKS $20 ¾ sticks $30 FULL STICKS $40". This item is, or appears to be, an illegal explosive device.

14. Your affiant was informed that KATTOUM was known by Milwaukee Police Department to be associated with "street takeover" events that have occurred throughout the city of Milwaukee. During these events there have been multiple instances of criminal activity. During a review of KATTOUM's publicly available Instagram account described above, your affiant observed at least one picture showing one of these street takeovers with the use of fireworks.



15. Your affiant found KATTOUM's publicly available Instagram account was linked to another Instagram account https://www.instagram.com/sauced.crew. The "sauced.crew" account was known to organize street takeover events in the city of Milwaukee and other locations.

16. On the same day, June 5, 2025, agents conducted in person surveillance at the TARGET RESIDENCE. Agents confirmed that the mailbox shown in the background of the

following picture belonged to 7356 S. Heatheridge Court, which is located across the street from TARGET RESIDENCE.

17. Agents confirmed that this mailbox belonged to 7356 S. Heatheridge Court, which is located across the street from TARGET RESIDENCE. This indicates the pictures of the illegal devices were taken inside the garage of the TARGET RESIDENCE.

18. Agents observed KATTOUM arrived in TARGET VEHICLE 1. He used a passcode to open the garage door and entered the garage.

19. In addition, agents were able to observe inside the garage from the street. They observed a stack of boxes which were covered by a grey tarp. The size, shape, and location was consistent with the boxes from above pictures.

20. You affiant reviewed the criminal history of KATTOUM. Your affiant found a valid protection order out of Milwaukee County (Milwaukee County case #2024FA006942) which showed it was related to a domestic violence incident.

21. As an ATF Special Agent, your affiant has conducted investigations of violations of Title 18 United States Code, Section 842(a)(3)(B), which makes it is unlawful to engage in the business of importing, manufacturing, or dealing explosive materials without a Federal explosives license issued by ATF. Furthermore, your affiant knows that it is a violation of Title 18, United States Code, Section 842(j) for any person to store any explosive materials in a manner not in conformity with Federal regulations. Such is the case when explosive materials are stored in an occupied residence. Further, your affiant has searched the relevant databases and found no evidence that KATTOUM has any license to manufacture, distribute, or store explosive materials.

5. Your affiant knows through training, knowledge and experience that illegal explosive devices are often constructed by persons who obtain certain chemicals, commonly called explosive precursor chemicals, through online of mail order. In their component form, these chemicals are not considered explosive materials and thus are not regulated by ATF. However, once combined or mixed, an explosive material commonly referred to as "flash powder" can be produced. Flash powder is classified as an explosive under Title 27, Code of Federal Regulations, Part 55, Subpart K, Section 55.201(a) and is thus subject to Federal manufacturing requirements. Flash powder is also subject to Federal explosives storage requirements as defined in Title 27 Code of Federal Regulations, Part 55, Subpart K. Flash powder devices can be small or large. Larger devices can blow up cars, homes, and be used to kill or maim individuals.

6. Your affiant knows that flash powder is used, by licensed persons, in the legal manufacture, distribution and use of explosives such as display fireworks. However, flash powder has also been used by unlicensed persons in the unlicensed, unregulated and unlawful manufacture of explosive devices for sale to or use by unlicensed persons in the general public. Persons who

manufacture such devices place flash powder into a container such as a sealed cardboard tube. A fuse or wick is inserted into the tube which is intended to be initiated with open flame. This wick is designed to burn to the point where it reaches the explosive contained inside the tube and whereby the explosive is initiated. Once initiated, the devices can explode with significant force. Unlike lawfully manufactured "commercial" explosives, which are generally designed to be insensitive to flame, these devices are considered "flame sensitive" and thus relatively easy for persons not specifically trained in the use of explosives to initiate. Furthermore, these explosive devices are made in a clandestine manner (in homes, barns, garages, etc.) with disregard to the safety of persons who may be residing nearby. Through their unlicensed and unregulated manufacture, sale and storage, these devices are referred to as "illegal explosive devices" by ATF.

DEFINITIONS ELECTRONICS

7. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs

and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. "Computer Server" or "Server" is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

d. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic,

magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include

encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (*e.g.*, external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (*e.g.*, computers, cellular telephones, and tablet devices such as an iPad).

i. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Media Access Control" ("MAC") address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number.

A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

k. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

8. I have consulted in this matter with lay persons and law enforcement officers who have specialized knowledge and training in computers, networks, and Internet communications. I have been informed that to properly retrieve and analyze electronically stored data, such as data on a computer, to ensure accuracy and completeness of such data, and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To effect such accuracy and completeness, it may also be necessary to

analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this warrant application seeks permission to search and seize records that might be found at or on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (*e.g.*, an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

9. Based on my knowledge, training, and experience, and after having consulted with SA Ludington, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;

b. the objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. the objects may be contraband or fruits of the crime.

10. I submit that if a computer or other electronic storage device is found on the premises ultimately authorized to be searched, there will also exist probable cause to believe that records falling within the list of items to be seized will be stored on that computer or other electronic storage device, for the following reasons, among others:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic storage device, the data contained in the file does not actually disappear. Rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media – in particular, computers' internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this

evidence because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

11. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might contain direct evidence of the crimes described in the warrant application, but also to locate evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

12. Although some of the records falling within the scope of items sought to be seized under requested warrant might consist of user-generated documents (such as word processor, picture, and movie files), many of those records might consist of electronic images, documents, records, or data on storage device storage media, for the reasons described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates on which files were created and the sequence in which the files were created.

b. Information stored within an electronic storage device and other electronic storage media might provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, and might thus enable the government to prove one or more elements of the suspected crime or crimes or, alternatively, to exclude an innocent suspect from further suspicion. In my training and experience, information stored within an electronic storage device (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs might indicate whether the electronic storage device was remotely accessed and might thus inculpate or exculpate the owner of the electronic storage device being searched. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs: computer user

account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external-device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the electronic storage device or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

13. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further,

in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require KATTOUM to press his finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. I am further aware several courts have held that compelling a suspect to provide his fingerprint to unlock a cell phone is non-testimonial and does not violate the 5th Amendment privilege against self-incrimination.

14. Based upon my knowledge, training and experience, and after having consulted with SA Ludington, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence is in the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect might try to conceal criminal evidence, or he or she might store it in random order with deceptive file names. Such actions by a suspect might require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process could take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

15. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to

contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals for this evidence on-site.

16. I know that when an individual uses a computer to commit crimes involving the search of how to manufacture explosives, build destructive and devices, and use those explosive devices, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The individual will often videotape themselves testing the explosive devices and store that video on their computer or phone. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

ATTACHMENT A

DESCRIPTION OF THE PROPERTY TO BE SEARCHED

- TARGET RESIDENCE: The Subject Premises is located at 7338 S. Heatheridge Court, Franklin, WI 53132, in the county of Milwaukee, in the eastern District of WI. It is a single-story-single family residence, white in color, with a grey roof. There is a front porch with brick/stone siding and an attached garage. The number ”7338” are prominently displayed vertically on the post of the porch next to the front door;
- TARGET VEHICLE 1: a white BMW, bearing Wisconsin license plate number, BAC-7291, registered to KATTOUM;

ATTACHMENT B

ITEMS TO BE SEIZED

Commercial and consumer 1.3 and 1.4 fireworks and explosive devices. Assembled improvised explosive devices, and unassembled components of these devices to include, but not limited to: metal, plastic or cardboard containers (i.e. pipe nipples, end caps, pvc pipe, cardboard tubes, bowls) or other containers; explosive filler material to include, but not limited to: powders (i.e., black powder, smokeless powder, pyrodex, flashpowder), pre-curser chemicals (potassium perchlorate, potassium chlorate, sulfur, aluminum powder) match heads, commercially manufactured high explosive materials (i.e., dynamites, slurries, emulsions), or unmixed chemical powders, substances or liquid chemicals that can be combined to produce an explosive material; chemicals used in the manufacture of explosives including but not limited to picric acid, aspirin, alcohol, sulfuric acid, potassium nitrate, peroxides, oxidizers, acetone, sodium nitrate, lead, wood alcohol, and unknown chemical residue if deemed to have been used in the manufacture of illegal explosive devices.

Mixing bowls, glassware or other containers, spoons, funnels or other mixing implements. commercially manufactured hobby fuse, colored fuse safety fuse, quick match, or other improvised fuse.

Literature pertaining to the assembly, manufacture and functioning of explosive devices or materials, including, but not limited to: books, pamphlets, drawings, sketches, diagrams, photographs, photocopies, computer generated or computer stored information of same; receipts showing the purchase of: componentry, chemicals/powders, tools, or literature, address books, phone lists, phone books or other notes containing associates, contacts or sources of supply; any items likely to be

contaminated or show traces of any chemicals or explosive materials, including but not limited to rugs, cushions, vacuum cleaner bags and attachments;

Any documents listing person's addresses, telephone numbers, or other contact information regarding the receipt, sale, purchase, storage, or theft of explosives;

Any pictures, photographs, or other images which include or may include images of firearms, ammunition, or explosives, any developed or undeveloped film, whether an original or copy, however produced, reproduced or stored, whether digitally, electronically, electro-magnetically, or otherwise, and each and every tangible thing from which images can be processed or recorded; indicia of property.

INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, or property designed or intended for use or which is or has been used to assist in obtaining the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 842(a)(3)(B) (distribution of explosives without an ATF license); and Title 18 United States Code, Section 842(j) (illegal storage of explosives):

1. Computers, cell phones, or storage media used as a means to or assist in obtaining the means of committing the violations described above.

2. For any computer, cell phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Records, information, and items relating to violations of the statutes described above including

a. Records, information, and items relating to the occupancy or ownership of the Subject Premises, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

5. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or

typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

6. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

7. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.